REMARKS

In the Office Action dated June 9, 2004, claims 1–18 were considered. The Office Action rejected claims 1–6, 8, and 10 under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,212,633 to Levy et al. ("Levy"), and rejected claims 7, 9, and 11–18 under 35 U.S.C. §103(a) as being unpatentable over Levy in view of U.S. Patent No. 5,889,958 to Willens ("Willens").

Applicants hereby amend the specification and the drawings to correct obvious grammatical errors and obvious errors in reference numbers. The Applicants respectfully submit that these amendments do not introduce new matter (MPEP §2163.07).

Applicants also hereby amend claims 1–18. The amendments to independent claims 1 and 10 are supported by the specification, for example by the Abstract of the Disclosure and at pages 2, 18, 19, and 25–29. Support for the amendments to independent claims 1 and 10 may also be found in the drawings, for example in FIGs. 6 and 7, and in the claims as originally-filed. Dependent claims 2–9 and 11–18 are amended to make their wording consistent with the wording of the independent claim from which they depend. Any required support therefor can be found in the specification, in the drawings, and in the claims as originally-filed.

Applicants hereby add new claims 19–26. The addition of claims 19, 22, 23, and 26 are supported by the specification, for example at pages 18, 19, and 25–29. The addition of claims 20 and 24 are supported by the specification, for example at page 5. The addition of claims 21 and 25 are supported by the specification, for example at pages 7, 18, and 19.

Applicants respectfully submit that no new matter is entered by the present amendments to claims 1–18 or by the addition of new claims 19–26. Upon entry of this paper, claims 1–26 will be pending in this application.

Rejection of Claims 1–6, 8, and 10 Under 35 U.S.C. §102(e)

Claims 1–6, 8, and 10 were rejected under 35 U.S.C. §102(e) as being anticipated by Levy.

Generally, Levy teaches "utilizing in conjunction with a memory-mapped serial communications interface a distributed firewall to permit secure data transmission between selected nodes over the interface. The distributed firewall incorporates security managers in the selected nodes that are respectively configured to control access to their associated nodes, thereby

restricting access to such nodes to only authorized entities. Moreover, . . . encrypted transmissions may be supported to restrict unauthorized viewing of data transmitted between the selected nodes over the interface" (Col. 3, lines 49–59).

The "memory-mapped serial communications interface . . . typically allocates a unified memory space to one or more nodes coupled to the interface, with each node having a portion of the memory space that is accessible by other nodes by referring to specific memory addresses within that allocated portion" (Col. 5, lines 41–47). The "interface is also serial in nature, thereby minimizing the number of physical wires defining the links between the nodes" (Col. 5, lines 53–55). The interface may be, for example, "implemented as an Institute of Electrical and Electronics Engineers (IEEE) specification IEEE 1394 (FireWire®) interface" (Col. 5, lines 56–58). FireWire® is a very fast, short-range, external serial bus used to connect various devices or nodes to one another and to a computer system.

The IEEE 1394 (FireWire®) interface disclosed in Levy is described to connect a plurality of local peripheral nodes to one another and to a computer system, and not to connect a local computer system to a remote computer system. For example, Levy discloses that "if a computer CPU is coupled to a video display and a DVD drive through an IEEE 1394 interface, the DVD drive could transmit video information directly to the video display over the interface, thereby eliminating the need for the CPU to process and oversee the transmission" (Col. 2, lines 45–50). As another example, Levy discloses that one may "couple a modem, a disk drive and a computer CPU together on a conventional IEEE 1394-based interface" (Col. 3, lines 22–24). Levy also states that "[o]ne example of a trusted interactive and directed node pair may be, for example, a computer and a disk drive" (Col. 11, lines 11–12).

As yet another example, FIG. 13 of Levy "illustrates one suitable layout for a plurality of nodes coupled to one another in a memory-mapped serial communications interface 300 consistent with the invention" (Col. 17, lines 14–17, and FIG. 13). A computer CPU node is connected to a plurality of other nodes, such as, for example, disks, a DVD ROM drive, a scanner, a printer, a set top box, a DVD, a television, a stereo, a digital audio tape, a VCR, and a camera (Col. 17, lines 24–40, and FIG. 13). The computer CPU node is also connected to a modem node, "e.g., a cable modem or other network-type interface" (Col. 17, lines 27–28).

In essence, Levy discloses a method of securely transmitting data among geographically

proximate (i.e., local) disk drives, video displays, DVDs, etc. using a very fast external serial bus (i.e., the IEEE 1394 (FireWire®) interface).

Amended Independent Claim 1

Applicants' amended independent claim 1 recites, in part, "establishing by a local computer system a network connection with a remote computer system" (emphasis added), and thereafter "receiving at the local computer system through the network connection an identifier from the remote computer system" (emphasis added). Moreover, as also recited in part in Applicants' amended independent claim 1, the received identifier is used "at the local computer system to filter information received through the network connection with the remote computer system" (emphasis added).

Levy fails to teach or suggest these limitations of Applicants' amended independent claim 1. Instead, as described above, Levy teaches using a memory-mapped serial communications interface (e.g., FireWire®) to connect a node, for example a computer CPU node, to a plurality of local peripheral nodes (Col. 17, lines 13–41, and FIG. 13). One of the plurality of local peripheral nodes may be, as described above, a modem node (e.g., a cable modem or other network-type interface), but Levy does not disclose using that modem node to establish a network connection between the computer CPU node and a remote computer system, thereafter receiving at the computer CPU node through the network connection an identifier from the remote computer system, and then using the identifier at the computer CPU node to filter information received through the network connection with the remote computer system.

Put another way, Levy's "distributed firewall" does not stop, or even address, unauthorized access or attacks upon an entire computer system. Instead, Levy's disclosure is limited to a much lower level, the device level, and to specifically addressed information available to serially connected, geographically proximate devices. In contrast, Applicants' claimed invention provides a true TCP/IP firewall, and extends its protection to entire computer systems which may or may not be geographically proximate. The claimed firewall prevents TCP/IP packets from infiltrating a protected network, and stops unauthorized accesses and attacks.

Accordingly, for at least these reasons, Applicants respectfully submit that amended

independent claim 1 is patentable over Levy.

Amended Independent Claim 10

Applicants' amended independent claim 10 recites, in part, "receiving at a local computer system a network connection from a remote computer system" (emphasis added), and thereafter "receiving at the local computer system through the network connection an identifier from the remote computer system" (emphasis added). Moreover, as in Applicants' amended independent claim 1, Applicants' amended independent claim 10 recites "using the identifier at the local computer system to filter information received through the network connection with the remote computer system" (emphasis added).

However, as discussed above with respect to Applicants' amended independent claim 1, Levy fails to teach or suggest the establishment of a network connection between a local computer system (e.g., the computer CPU node 302 of FIG. 13) and a remote computer system by using, for example, the modem node 310 of FIG. 13, and thereafter receiving at the local computer system through the network connection an identifier from the remote computer system for use in filtering, at the local computer system, information received through the network connection with the remote computer system.

Accordingly, for at least these reasons, Applicants respectfully submit that amended independent claim 10 is also patentable over Levy.

Dependent Claims 2–6 and 8

Because claims 2–6 and 8 depend directly from amended independent claim 1, Applicants respectfully submit that these claims are also patentable over Levy.

Accordingly, Applicants respectfully request that the rejection of claims 1–6, 8, and 10 under 35 U.S.C. §102(e) as being anticipated by Levy be reconsidered and withdrawn.

Rejection of Claims 7, 9, and 11–18 Under 35 U.S.C. §103(a)

Claims 7, 9, and 11–18 were rejected under 35 U.S.C. §103(a) as being unpatentable over Levy in view of Willens.

Generally, Willens teaches systems and processes which use "dynamically down-loadable user specific filters from a central server for content monitoring and user authorization in a

network of networks" (Col. 1, lines 9–12). More particularly, Willens teaches "an Internet access system 10 which incorporates an access control subsystem 12" (Col. 3, lines 54–55). "The access control subsystem 12 is implemented with a communications server 14, one or more Remote Authentication Dial In User Service (RADIUS) servers 16, and a remote access server 18" (Col. 3, lines 56–59).

A user 22 at a first computer system may log in through the communications server 14, i.e., a second remotely located computer system (Col. 5, lines 9–10, and FIG. 3). The RADIUS server 16 may provide a filter identification to the communications server 14 (Col. 5, lines 14–18). Client software 44 resident on the communications server 14 then checks to see if the identified filter is stored locally in the communications server's cache 50. (Col. 5, lines 18–20). "If it is, the client software 44 uses it for controlling access. If not, the client software 44 sends a lookup request to the network access server 18 . . . to download the filter[,] . . . which is maintained in the server 14 memory for the rest of the user 22's session." (Col. 5, lines 20–26).

A user profile 46, which identifies the appropriate filter, is resident on the access control system 12 (e.g., on the RADIUS server 16 of the access control system 12) (Col. 5, lines 10–13, and FIG. 3). Moreover, "[i]n practice, the client software 44 and permit-based filtering technology is integrated in the communications operating system software that runs on the server 14" (Col. 5, lines 34–36).

In essence, Willens discloses a simple content filter which prevents users inside a firewall from accessing impermissible content outside the firewall.

Willens Fails to Remedy the Deficiencies of Levy

Applicants' claims 7, 9, and 11–18 depend directly or indirectly from either amended independent claim 1 or amended independent claim 10. Moreover, each one of those dependent claims incorporates all of the limitations of the independent claim from which it depends. Applicants' amended independent claims 1 and 10 each recite, in part, "receiving at the local computer system through the network connection an identifier from the remote computer system" and "extending the firewall by using the identifier at the local computer system to filter information received through the network connection with the remote computer system."

Willens fails to teach or suggest at least these limitations of Applicants' amended

independent claims 1 and 10. Specifically, the user 22 in Willens does not receive through the network connection established with the communications server 14 an identifier from the communications server 14 for use in filtering information received through that network connection. Similarly, the communication server 14 does not receive through the network connection established with the user 22 an identifier from the user 22 for use in filtering information received through that network connection. Rather, as described above, the user profile 46 that identifies the appropriate filter, the client software 44 that uses the identified filter to control access, and the permit-based filtering technology is all already resident on the access control system 12. Thus, Willens does not disclose, or even allow for, the secure network (or firewall) extension of Applicants' amended independent claims 1 and 10. Willens, therefore, fails to remedy the deficiencies of Levy.

To summarize, Willens, in a similar fashion to Levy, does not disclose stopping attacks upon the entire computer system of the user 22, and does not teach the extension of a firewall to the user 22, as required by Applicants' amended independent claims 1 and 10. Instead, as mentioned, Willens discloses a simple content filter which prevents users inside a firewall from accessing impermissible content outside the firewall.

The Proposed Combination of Levy and Willens is Improper

According to MPEP §2143, to establish a prima facie case of obviousness, "there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings."

Levy discloses a method of securely transmitting data among geographically proximate (i.e., local) devices or nodes (e.g., disk drives, video displays, DVDs, etc.) using a very fast external serial bus (i.e., the IEEE 1394 (FireWire®) interface). Willens, on the other hand, relates to techniques for Internet content control that prevent a user inside a firewall from accessing impermissible content outside the firewall. However, Levy's FireWire® interface, which is used to communicate at the local device level, would be incapable of implementing the network communications between the remotely located computer systems that Willens describes. Simply put, FireWire® is an inappropriate media for implementing network communications between

two geographically distant computer systems.

Accordingly, there is no suggestion or motivation to modify or combine the cited references. Moreover, even if one were to modify or combine Levy and Willens, one would not, for at least the reasons described above, arrive at the Applicants' claimed invention.

Applicants, therefore, respectfully submit that claims 7, 9, and 11–18 are patentable over Willens, either alone or in proper combination with Levy. Accordingly, Applicants respectfully request that the rejection of claims 7, 9, and 11–18 under 35 U.S.C. §103(a) be reconsidered and withdrawn.

Newly Added Claims 19–26

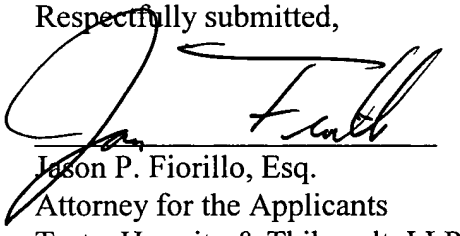
Applicants' newly added claims 19–26 depend directly or indirectly from either amended independent claim 1 or amended independent claim 10. As each one of these newly added dependent claims incorporates all of the limitations of the independent claim from which it depends, Applicants respectfully submit, for at least the reasons set forth above, that claims 19–26 are allowable as well.

CONCLUSION

Claims 1–26 are pending in the application. Applicants request that the Examiner reconsider the application and claims 1–26 in light of the foregoing Amendment and Response, and respectfully submit that the pending claims are in condition for allowance. Accordingly, Applicants respectfully request withdrawal of all grounds of rejection, and allowance of claims 1–26 in due course.

If, in the Examiner's opinion, a telephonic interview would expedite the favorable prosecution of the present application, the undersigned attorney would welcome the opportunity to discuss any outstanding issues, and to work with the Examiner toward placing the application in condition for allowance.

Respectfully submitted,



Date: November 9, 2004
Reg. No.: 52,892
Tel. No. (617) 310-8471
Fax No. (617) 248-7100

Jason P. Fiorillo, Esq.
Attorney for the Applicants
Testa, Hurwitz & Thibeault, LLP
High Street Tower
125 High Street
Boston, MA 02110

3132979

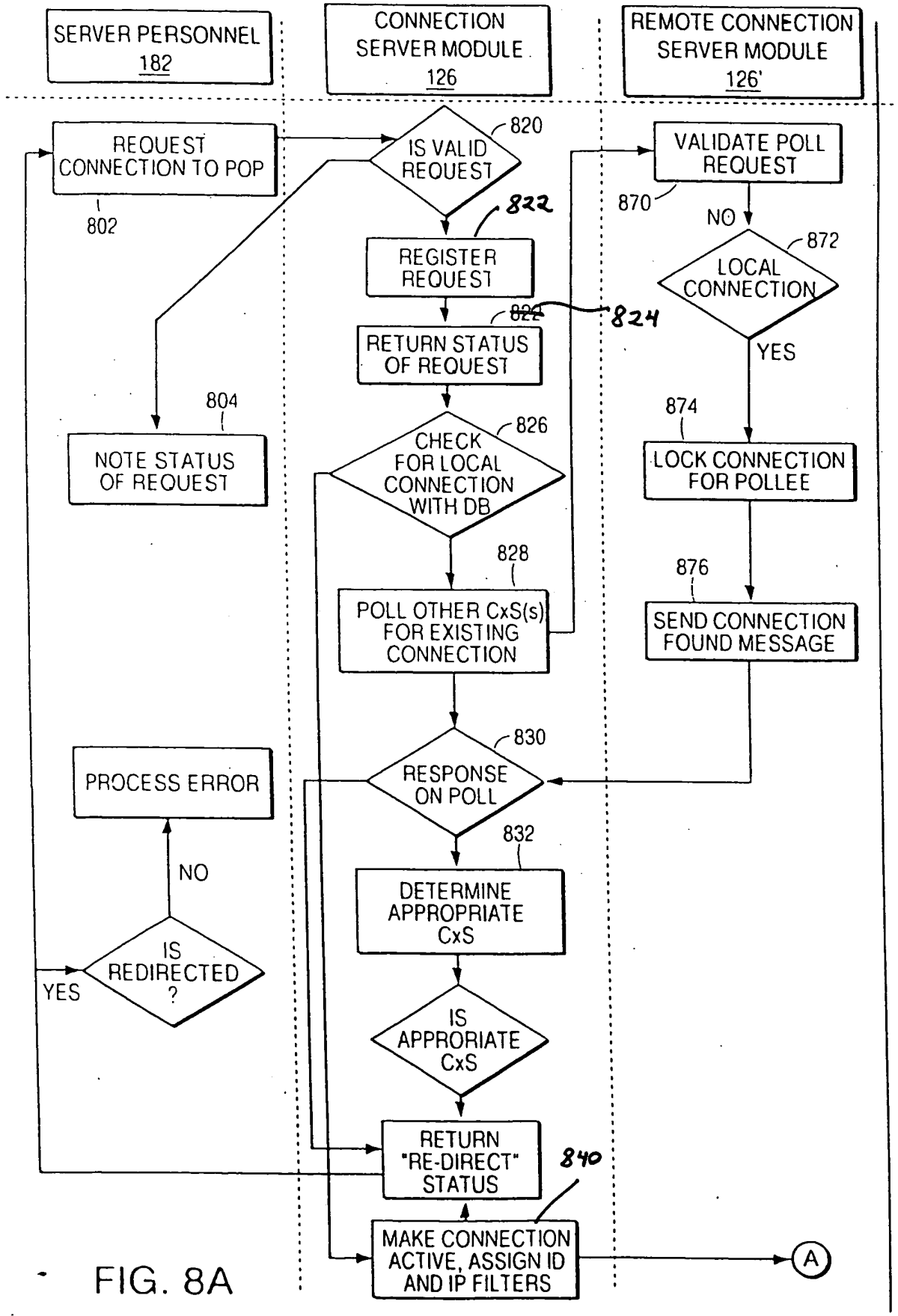


FIG. 8A

Annotated Marked-Up Drawing

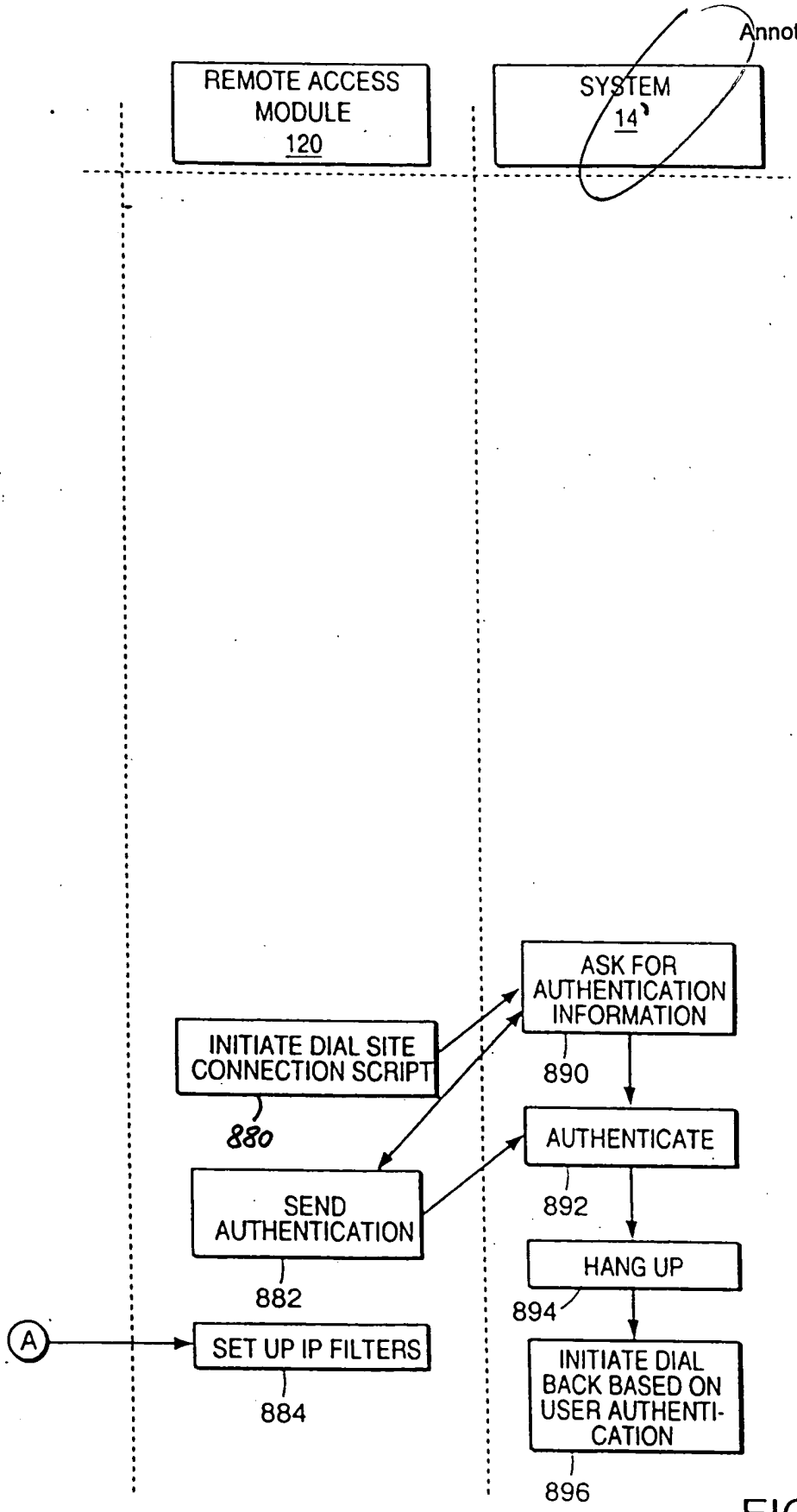


FIG. 8B